

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Comment Sought on Privacy and Security of)	CC Docket No. 96-115
Information Stored on Mobile Communications)	
Devices)	
)	DA 12-818
)	

REPLY COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200

July 30, 2012

TABLE OF CONTENTS

	<u>PAGE</u>
I. INTRODUCTION AND SUMMARY	1
II. COMMENTERS WIDELY AGREE THE COMMISSION SHOULD NOT REGULATE DATA STORED ON MOBILE DEVICES.....	2
III. SECTION 222 DOES NOT AUTHORIZE THE COMMISSION TO REGULATE WIRELESS PROVIDERS WHEN THEY RETRIEVE INFORMATION STORED ON WIRELESS DEVICES BECAUSE SUCH INFORMATION IS NOT CPNI.	6
IV. CONCLUSION.....	12

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Comment Sought on Privacy and Security of)	CC Docket No. 96-115
Information Stored on Mobile Communications)	
Devices)	
)	DA 12-818
)	

REPLY COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

I. INTRODUCTION AND SUMMARY

CTIA – The Wireless Association® (“CTIA”) hereby respectfully submits its reply comments in the above-captioned proceeding.¹ The opening comments reflect broad agreement among wireless stakeholders that the Commission should not adopt new rules under Section 222 of the Communications Act that would limit wireless carriers’ use of network diagnostic tools to improve wireless voice and data service. As many commenters explained, such rules are unnecessary and would actually harm consumers by restricting providers’ ability to improve service quality. Commenters also widely agree that regulating data stored on mobile devices in today’s “open” Internet environment would be ineffective and counterproductive because wireless carriers today are not gatekeepers for wireless customers. Accordingly, commenters have urged the Commission to allow the NTIA to develop a comprehensive and flexible approach to these privacy issues.

Wireless stakeholders are similarly skeptical about the Commission’s statutory authority under Section 222 to regulate carriers’ use of tools to diagnose and troubleshoot network

¹ *Comment Sought On Privacy And Security Of Information Stored On Mobile Communications Devices*, Public Notice, CC Docket No. 96-115, DA 12-818 (May 25, 2012) (“Public Notice”).

problems in order to improve the provision of service to subscribers. The record shows that data stored on mobile devices is *not* CPNI within the meaning of Section 222 because it is not “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service.”² The New America Foundation’s claim that the Commission should find in Section 222 a roving mandate for the agency to safeguard the privacy of all types of data stored on wireless devices lacks any textual basis in the limited congressional delegation over consumer privacy in the statute.

II. COMMENTERS WIDELY AGREE THE COMMISSION SHOULD NOT REGULATE DATA STORED ON MOBILE DEVICES.

As CTIA explained, the Commission should not, as a matter of policy, attempt to regulate the storage of customer data on mobile devices.³ Commenters agree that any effort to regulate in this area would be ineffective in today’s environment, and inconsistent with the objective of an open Internet. Moreover, as the Commission has recognized, wireless carriers need flexibility to use stored data for network diagnostic purposes for the ultimate goal of improving wireless service. NTIA is already considering these privacy issues as part of a broader, ongoing multi-stakeholder process that involves the wireless industry as well as many other stakeholders who filed comments in this proceeding. Commenters widely agree that the Commission should not attempt to duplicate or get out ahead of this process.

The record shows that consumers use a variety of applications and other third-party software to store personal data on their mobile devices, providing many other players in the wireless ecosystem with the ability to access this information. “In today’s open Internet environment, a variety of players—including mobile service providers, device manufacturers,

² 47 U.S.C. § 222(h)(1).

³ Comments of CTIA – The Wireless Association at 3-6, CC Docket No. 96-115 (July 13, 2012).

operating systems, application developers, browsers, software developers—have access to information stored on devices in order to provide a variety of innovative new products and services to consumers.”⁴ All of these players “provide services directly to consumers over their wireless devices” and are “forming customer relationships based on mobile services.”⁵ “[B]ecause consumers are largely free to use the apps they desire, without interference by the service provider, the service provider in turn is necessarily precluded from playing any meaningful ‘gatekeeper’ role with respect to consumer privacy.”⁶ In this environment, regulating the practices of network providers would be an ineffective way to protect consumer privacy.⁷

⁴ Comments of Verizon Wireless at 1, CC Docket No. 96-115 (July 13, 2012); *see also* Internet Commerce Coalition Comments at 3, CC Docket No. 96-115 (July 13, 2012) (explaining that customer information “may be available to a broad range of application providers and other actors in the mobile eco-system who have no relationship with carriers”); Interactive Advertising Bureau Comments at 2, 5, CC Docket No. 96-115 (July 13, 2012) (“The mobile marketplace is no longer limited to service providers and handset manufacturers. . . . The wireless service provider and handset manufacturer are no longer the only parties or entities with access to information that relates to the mobile device or the consumer’s use of the device[.]”); Consumer Electronic Association Comments at 3-4, CC Docket No. 96-115 (July 13, 2012).

⁵ Comments of AT&T at 1, 6, CC Docket No. 96-115 (July 13, 2012).

⁶ Verizon Comments at 4; *see also* Comments of Sprint Nextel Corp. at 9, CC Docket No. 96-115 (July 13, 2012) (“Carriers are no longer the gatekeepers or sole enablers of the mobile experience.”); AT&T Comments at 6-8.

⁷ AT&T Comments at 8-9; *see also* Sprint Nextel Comments at 2 (“Requiring carriers to be responsible for the security and privacy of all data on mobile devices would be unworkable and beyond a carriers’ capabilities due to lack of carrier design, control, or physical custody of users’ devices or insight into what data a particular user may actually have on the users’ device.”); Internet Commerce Coalition Comments at 3 (“Thus, imposing privacy and security regulation by means of the CPNI statute, far from focusing on an issue unique to carriers, is addressing a broader issue, and doing so in an asymmetrical and under-inclusive way.”).

Regulation would also be counterproductive. Third-party access to and use of this stored data results from the open Internet the Commission advocates.⁸ “The popularity of data services and mobile applications has revolutionized what consumers expect from their mobile devices. Mobile devices are no longer viewed solely, or perhaps even primarily, as a vehicle for traditional telecommunications services offered by the mobile provider.”⁹ As Verizon Wireless explained, “[t]oday’s smartphones, tablets and other IP-enabled devices are operationally similar to computers and are thus far different from mobile devices available even just a few years ago.”¹⁰ Regulating data stored on mobile devices would run counter to consumers’ demand for the same latitude to install third-party software, services, and applications on their mobile devices that they enjoy on their home computers. Indeed, carriers provide their consumers with wide latitude to download apps and software that may access their data, and wireless users have the same expectations for their mobile devices.¹¹

Moreover, commenters agree that there are many acceptable uses of data stored on mobile devices. Most notably, wireless carriers use network diagnostic information stored on mobile devices to improve wireless voice and data service. As AT&T explained, “[t]hese data have been invaluable to AT&T in improving its network and the services it offers to its customers.”¹² And as Sprint Nextel further explained, “collection of diagnostic data from

⁸ See Interactive Advertising Bureau Comments at 2 (“The mobile Internet economy flourished thanks to an open environment built on choice: multiple platforms, operating systems, applications, and browsers placed exciting content and services at the consumer’s fingertips.”).

⁹ AT&T Comments at 6.

¹⁰ Verizon Comments at 1; *see also* Sprint Nextel Comments at 1-2 (“Mobile devices have an ever-expanding capacity to serve as ‘smart’ information systems while delivering telephone services.”).

¹¹ Verizon Comments at 5; Sprint Nextel Comments at 3-4.

¹² AT&T Comments at 19.

handsets, in addition to network diagnostic data, is beneficial to our customers and helps carriers provide the services customers expect.”¹³ Network diagnostic tools ultimately benefit consumers, and their use should not be discouraged by the Commission. Restricting or forbidding the use of these tools would harm consumers by hamstringing providers in their ability to improve service quality with the limited spectrum capacity currently available.¹⁴

In light of these concerns, wireless stakeholders have urged the Commission to allow the NTIA to lead the way in developing a comprehensive and flexible privacy framework.¹⁵ “Given the wide range of industry participants collecting and using customer data, a single, comprehensive approach that encompasses all mobile services would be far superior to a piecemeal regulatory approach in which individual agencies impose different rules for whichever small slice of data falls within their jurisdictions.”¹⁶ Indeed, the concerns that the FCC raises are a small subset of a broader, more complex issue—namely, how to best protect consumers in an Open Internet environment.¹⁷ NTIA is already considering these privacy issues as part of a

¹³ Sprint Nextel Comments at 2; *see also id.* at 6-7; Comments of the Telecommunications Industry Association at 7, CC Docket No. 96-115 (July 13, 2012) (“The use of consumer information to design products and improve services, as well as to fund free services and content, has produced substantial benefits for consumers.”).

¹⁴ Telecommunications Industry Association Comments at 4 (“Care should be taken in order to avoid developing overly prescriptive rules for the maintenance and use of customer data.”).

¹⁵ *See* Verizon Comments at 1, 6, 9-10; AT&T Comments at 8-13; Comments of the Alliance for Telecommunications Industry Solutions at 1, CC Docket No. 96-115 (July 13, 2012); Consumer Electronics Association Comments at 11-12; Comments of TechAmerica at 4, CC Docket No. 96-115 (July 13, 2012); Comments of Information Technology and Innovation Foundation at 4, CC Docket No. 96-115 (July 13, 2012).

¹⁶ AT&T Comments at 8.

¹⁷ *See* Internet Commerce Coalition Comments at 2 (explaining that “expanding CPNI regulation and the concept of CPNI itself to attempt to address this issue would regulate a sliver of the complex mobile eco-system in a way that would be asymmetrical, ineffective and inappropriate”).

broader, ongoing multi-stakeholder process that involves the wireless industry.¹⁸ “A code of conduct, such as that under consideration in NTIA’s multi-stakeholder process, is the best method to address these issues.”¹⁹ Rather than launch a duplicative process, the Commission should await the result of the NTIA’s process before considering any new rules in this area that could inadvertently harm the very consumers it seeks to protect.²⁰

III. SECTION 222 DOES NOT AUTHORIZE THE COMMISSION TO REGULATE WIRELESS PROVIDERS WHEN THEY RETRIEVE INFORMATION STORED ON WIRELESS DEVICES BECAUSE SUCH INFORMATION IS NOT CPNI.

The record also clearly shows that Section 222 does not authorize the Commission to regulate network diagnostic information and other information acquired from wireless devices.²¹ Under Section 222, CPNI is “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship” and “information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”²² As CTIA explained, data stored on mobile devices does not come within the definition of CPNI.²³ The Stored Communications Act confirms the Commission’s lack of

¹⁸ See AT&T Comments at 1-2.

¹⁹ Verizon Comments at 2; *see also id.* at 9-10; Telecommunications Industry Association Comments at 8-13.

²⁰ Consumer Electronics Association Comments at 12.

²¹ CTIA Comments at 6-10; Sprint Nextel Comments at 11-14; Verizon Comments at 8; Internet Commerce Coalition at 3; Consumer Electronics Association Comments at 4-9; Interactive Advertise Bureau Comments at 5-8.

²² 47 U.S.C. § 222(h)(1).

²³ CTIA Comments at 6-10.

statutory authority to restrict wireless carriers' use of network diagnostic information.²⁴

The New America Foundation's claim that data stored on mobile devices is CPNI lacks merit.²⁵ It claims that data stored on mobile devices is CPNI under both § 222(h)(1)(A) and (B) because it is similar to the "detailed call, text, and data logs" that carriers provide "through their web pages."²⁶ This argument has no textual support in Congress's limited delegation to the Commission of authority over consumer privacy in Section 222. Moreover, much of the data stored on mobile devices has no connection with a CMRS carrier. Not only can data be sent and received using WiFi and other non-CMRS services, but data contained on a smart phone or tablet can include pictures and data associated with downloadable applications, *e.g.*, music files, contact lists for interactive games, et cetera. Section 222 does not provide the FCC with general authority to regulate privacy practices; it only governs defined information that is acquired in a specific manner by telecommunications carriers.

Contrary to New America Foundation's claim, network diagnostic information does not meet the definition of CPNI in § 222(h)(1)(A) because it is not personally identifiable. The statute reflects Congress's intent that only "individually identifiable" information be strictly regulated as CPNI.²⁷ As the Commission has explained, "Congress accorded CPNI—which includes personal, individually identifiable information—the greatest level of protection."²⁸

²⁴ *Id.* at 10-11; Sprint Nextel Comments at 14.

²⁵ Comments of New American Foundation's Open Technology Institute *et al.* at 2-4, CC Docket No. 96-115 (July 13, 2012).

²⁶ *Id.* at 2.

²⁷ 47 U.S.C. § 222(c)(1).

²⁸ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, ¶ 7 (2002).

Regardless of whether “call, text, and data logs” may be personally identifiable, network diagnostic information is not because it does not relate to any particular customer.²⁹ As Sprint Nextel explained, network diagnostic data does “not involve individual handset or individual user activities, nor are the types of data collected sensitive or particularly impactful on privacy.”³⁰ “The purpose of remote diagnostic data collection is not to analyze individual consumers’ usage, and the reports generated by carriers could not be used to create a detailed picture of a specific customer’s usage.”³¹ Rather, it is generalized information that relates to the performance of the network and allows wireless carriers “to provide a better network for *all* customers.”³²

Nor does network diagnostic information meet the definition of CPNI in § 222(h)(1)(B). Detailed information on why a call was dropped or why an application failed is not information “contained in the bills” of a customer. Even if it were, this information does not “pertain[] to telephone exchange service or telephone toll service” when it relates to failed data or application

²⁹ Moreover, a customer’s name, address, and telephone number is not covered by the definition of CPNI; to the contrary, carriers are required to make this information available. *See* 47 U.S.C. § 222(e) and (h).

³⁰ Sprint Nextel Comments at 2; *see also id.* at 7 (“Sprint’s general experience in the use of diagnostics data collection from handsets, as reported previously, has not been customer-specific; rather, Sprint has developed and used reports of de-identified device information and aggregated data to understand group performance situations and design solutions for network enhancements. This is not sensitive or personal information collected on the handset and it is generally not CPNI-related. What Sprint has learned from sampling a pool of diagnostic metrics from devices in particular locations or with particular problems at set times is that we are collecting data that may be relevant not to a single customer, but across our customer base.”); *id.* at 12 (“In addition, the data collected from devices is usually device specific, and not consumer specific. Meaning, the information is collected about how a device functioned and is not linked to individual users.”).

³¹ *Id.* at 12-13.

³² AT&T Comments at 20 n.56.

sessions.³³ “Indeed, the plain language of the statute demonstrates that Congress did not intend for the FCC to extend its regulatory purview to information services such as those involved in mobile data communications.”³⁴

Other data stored on mobile devices—*i.e.*, pictures, texts, emails—may be personal to consumers but are not call data regulated as CPNI under Section 222.³⁵ “Generally speaking, most of the data on the device is either entered into the device by consumers or generated through a consumer’s interaction with a mobile app” and does “not relate to a customer’s use of a telecommunications service.”³⁶ As CTIA explained, this information does not “relate[] to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier.”³⁷ Moreover, “[i]nformation stored on the device that is collected or transmitted by applications or the mobile operating system is not *made available to the carrier by the customer solely by virtue of the carrier-customer relationship*.”³⁸ Nor is this “information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”³⁹

³³ 47 U.S.C. § 222(h)(1)(B).

³⁴ Interactive Advertising Bureau Comments at 5.

³⁵ CTIA Comments at 9-10; Sprint Nextel Comments at 13-14; Information Technology and Innovation Foundation Comments at 1; Interactive Advertising Bureau Comments at 5-8.

³⁶ Sprint Nextel Comments at 12-13.

³⁷ 47 U.S.C. § 222(h)(1)(A).

³⁸ Consumer Electronics Association Comments at 7 (emphasis in original); *see also* Sprint Nextel Comments at 13 (“First, most information stored by customers on their devices is not made available to carriers. With the proliferation of smart phones and downloadable apps, there are an endless number of companies that can connect with customers through their mobile devices. While certain companies can collect data about customers through use of apps, the data is not generally available to carriers. Carriers may have access to certain data on devices; e.g., the remote diagnostic data discussed above; but carriers do not collect all data stored on a device.”).

³⁹ 47 U.S.C. § 222(h)(1)(B).

Acceptance of New America Foundation’s arguments would lead to the very sort of vast, unconstrained authority over personal consumer data—from emails and texts to pictures and tweets—that, as CTIA observed in its comments, are clearly outside the Commission’s reach under Section 222.⁴⁰

Even if this information were CPNI, which it clearly is not, Section 222 expressly permits wireless providers to use the data in order to improve wireless service and customer care.⁴¹ For example, a wireless provider “that receives or obtains” CPNI “by virtue of its provision of a telecommunications service” may “use, disclose, or permit access to individually identifiable” CPNI “in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service.”⁴² The Stored Communications Act confirms the Commission lacks authority to restrict

⁴⁰ CTIA Comments at 9-10; *see also* Consumer Electronics Association Comments at 5 (“In contrast, the FCC only has jurisdiction over specific aspects of information privacy and lacks the broad cross-industry data privacy enforcement experience of the FTC. . . . Section 222, however, does not provide the FCC with general authority to regulate privacy practices – it only governs defined information that is acquired in a specific manner by telecommunications carriers. . . . The FCC thus does not have general authority to regulate privacy practices beyond the protections found in Section 222, which covers a shrinking part of the services and providers in the mobile marketplace.”); Interactive Advertising Bureau Comments at 7 (“A broadened reading of the definition of CPNI would result in an expansion of the Section 222(c) duty beyond its intended and stated purpose to protect the confidentiality of individually identifiable proprietary information, and reach into all information collected by a carrier on a mobile device.”); Information Technology and Innovation Foundation Comments at 1 (“The FCC’s proposed interpretation is not valid based on a close reading of Section 222(h)(1). The text is clear that the CPNI clause only covers specific types of information collected by carriers, not all possible customer information. Moreover, it certainly does not extend to the mechanisms that may be used to collect information. If it did, then this would suggest the FCC could, under this authority, regulate every aspect of the device that collects input including microphones, keyboards, touch screens, and any other sensor.”).

⁴¹ *See* Public Notice at 3 (acknowledging that the data is used for “network diagnostics or improving customer care”).

⁴² 47 U.S.C. § 222(c)(1); *see also* 47 U.S.C. § 222(d)(1), (2); AT&T Comments at 20 n.56; Sprint Nextel Comments at 14.

the use of network diagnostic information for this purpose.⁴³

The New America Foundation does not dispute that carriers' use of network diagnostic information is permitted by § 222. Rather, they claim that the Commission should collect "more detailed information" about carrier practices because they have the "incentive" to collect CPNI "for a variety of purposes beyond network and service improvement."⁴⁴ That is not a legal argument, and there is no basis for their bald speculation that carriers use CPNI for purposes other than those permitted by § 222. Its desire for a "more robust record" would not cure the absence of Commission authority to regulate in this area.⁴⁵

⁴³ 18 U.S.C. § 2702(c)(2), (3), (6).

⁴⁴ New American Foundation Comments at 5.

⁴⁵ *Id.* at 8.

IV. CONCLUSION

Wireless stakeholders broadly agree that the Commission lacks statutory authority to regulate in this area and should not adopt any new rules that would restrict carriers' ability and legitimate right to use network diagnostic software to collect information that will improve wireless voice and data services. NTIA is considering these privacy issues as part of a broader, ongoing multi-stakeholder process that involves the wireless ecosystem and other stakeholders who filed comments in this proceeding. Rather than launch a duplicative proceeding, the Commission should await the result of that process.

Respectfully submitted,

By: *Krista L. Witanowski*

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA – The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200

Dated: July 30, 2012